Surveillance et vie privée

Forget, Catherine; Dumortier, Franck; Vanmeerbeek, Perrine; Lazaro, Christophe; Grandjean, Nathalie; Loute, Alain

Published in:
Kairos

Publication date:
2016

Document Version
le PDF de l'éditeur

SURVEILLANCE ET VIE PRIVÉE:
À LA RECHERCHE DE L'ENNEMI INTÉRIEUR

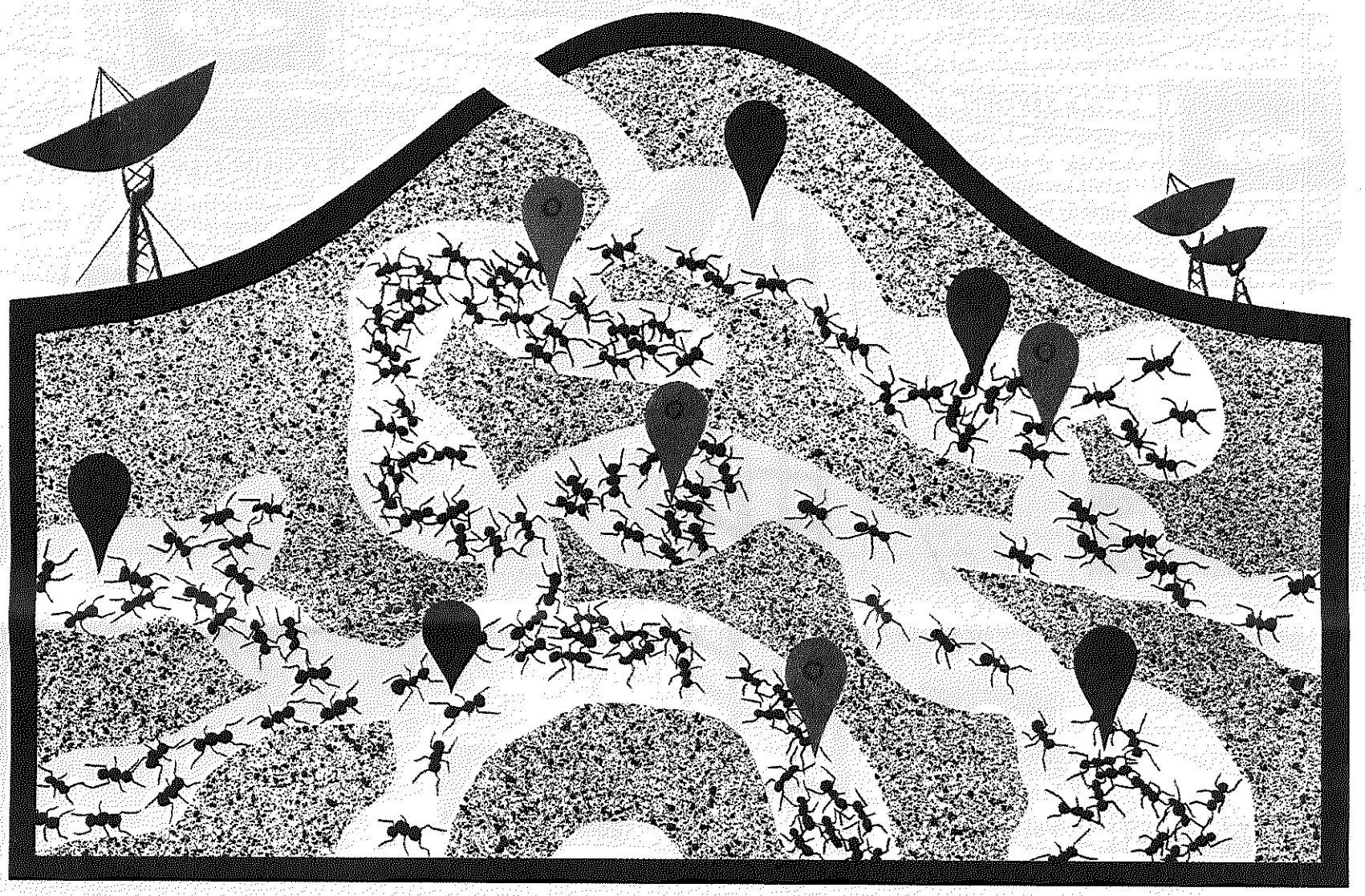


Illustration: Eponine Cottey

Même si le fichage des personnes à des fins de contrôle ne date pas d'hier, les nouvelles technologies facilitent la possibilité de traiter davantage de données d'un plus grand nombre de personnes, au grand dam des droits fondamentaux. A titre illustratif, le Parlement européen estime la surveillance de masse disproportionnée, qu'importent les garanties mises en œuvre par les États. Selon ce dernier, «*le respect de la vie privée n'est pas un droit de luxe, mais constitue la pierre angulaire de toute société libre et démocratique; il souligne par ailleurs que la surveillance de masse a des répercussions potentiellement graves sur la liberté de la presse, la liberté de pensée et la liberté d'expression, ainsi que sur la liberté de réunion et d'association, et qu'elle entraîne un risque élevé d'utilisation abusive des informations collectées à l'encontre d'adversaires politiques*»[1].

Le terme surveillance de masse est particulièrement flou eu égard au nombre de dispositifs susceptibles d'être concernés: banque de données policières, caméras de surveillance, rétention de données... Ce dossier a donc pour objectif de passer en revue les dernières mesures adoptées ou en voie de l'être, afin de faire un tour d'horizon de certaines techniques mises en place par les États de l'Union européenne et plus particulièrement, la Belgique.

Tout d'abord, la Banque de données Nationale Générale fait régulièrement une sortie médiatique, les journalistes pointant le nombre important de personnes «fichées». En effet, cette banque de données alimentée par les services de police, comprend toute information pertinente, soit potentiellement toute information. Même si le fichage d'un fait anodin «*n'a pas à faire craindre qui n'a rien à cacher*», le risque d'abus et d'accès illicite voire arbitraire à ces données est bien présent (p.10-11). Outre «l'Oeil de Sauron» pour reprendre les termes de l'auteur, nos rues sont garnies de caméras intelligentes susceptibles de détecter des mouvements «suspects». Or, leur efficacité est loin d'être démontrée (p.12-13).

Ensuite, dans l'environnement numérique, le panel de mesures ne cesse de s'intensifier (*Passager Name Record, rétention de données*... (p.14-15)). Tandis que nous crions au loup, certaines entreprises fournissant des services gratuits type Facebook ou Google, traitent nos données, les croisent et les transforment en véritable source de profits. Ces données constituent également une mine d'informations pour les autorités répressives, les acteurs privés étant tributaires d'une obligation de collaboration envers les enquêteurs. La surveillance de masse n'est donc pas que répressive, elle est aussi et tout d'abord commerciale (p.15-16). Néanmoins, si le sentiment d'impuissance est bien présent face à des technologies que nous ne maîtrisons pas ou peu, la résistance s'organise venant mettre à mal ce présupposé transfert consenti de données à caractère personnel sur la toile (p.16-17).

Enfin, de manière transversale, l'ensemble de ces dispositifs revêtent un caractère «numérique» et incluent de nouvelles fonctions: détection, *tracking*, identification, géolocalisation... La surveillance n'est plus que matérielle, elle est aussi virtuelle. Entre adoucissement et intensification du contrôle, la surveillance technologique n'en est pas moins toujours plus invasive (p.18-19).

Les nouvelles technologies représentent également de réels enjeux sociétaux. Si certains sont à la recherche de leur for intérieur, d'autres sont surtout à la recherche de l'ennemi intérieur. Surfant sur un discours de lutte contre le terrorisme et invoquant le «problème» de l'immigration, un État «ultra préventif» se développe, au bonheur des sociétés et du lobby sécuritaires.

Dossier coordonné par Catherine Forget

(1) Rapport du 21 février 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188(INI)), point 10, disponible sur http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//FR.

LA BANQUE DE DONNÉES NATIONALE GÉNÉRALE : L'ŒIL DE SAURON ?

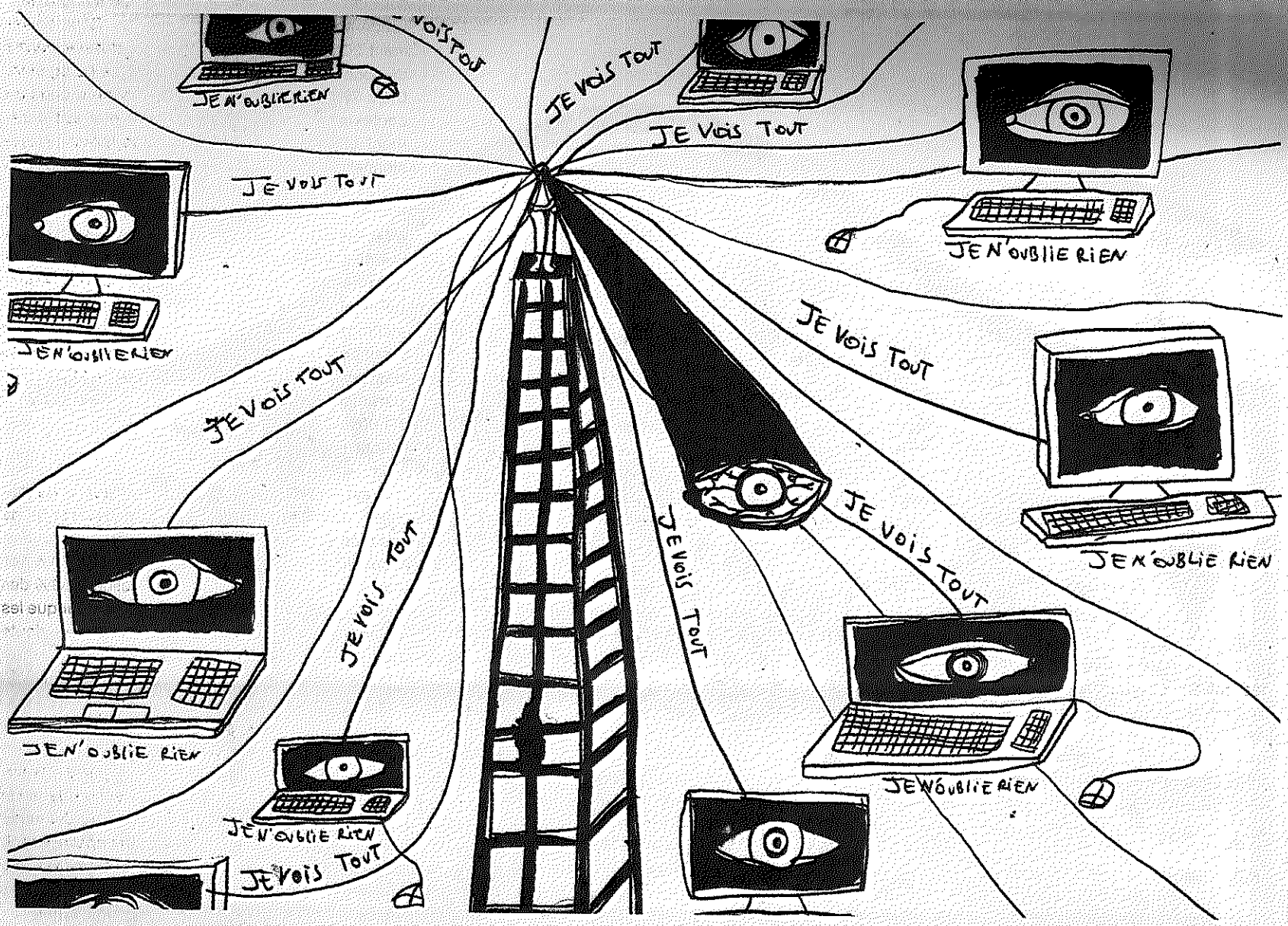


Illustration: Priscilla Beccari

Lors d'un contrôle d'identité, il est fréquent que des quidams s'entendent dire qu'ils sont déjà «*connus*» des services de police, parfois même lorsque leur casier judiciaire est vierge. A l'inverse, les personnes contrôlées n'ont souvent aucune connaissance des informations dont elles font l'objet et ne peuvent donc pas s'en défendre. Lors d'un simple contact avec les autorités, de nombreuses personnes sont ainsi «*profilées*» à leur insu et ont de fortes chances d'être discriminées dans leurs rapports avec celles-ci. L'origine des informations dont disposent les forces de l'ordre s'explique, bien entendu, par le fait que celles-ci ont, à tout moment, la possibilité de consulter une nébuleuse de bases de données dont la gestion est articulée autour de la Banque de données Nationale Générale (ci-après «BNG») qu'elles ont l'obligation d'alimenter au risque de poursuites pénales. D'après les chiffres disponibles – extrêmement opaques, puisque non publiés officiellement in extenso depuis 2008[1] – le succès du système est tel qu'il semble qu'une personne sur six en Belgique soit actuellement fichée. Au 31 décembre 2012, 1 769 439 personnes y figuraient. Afin de faciliter la collecte de données au sein de la BNG, un flux électronique a été mis en place afin que celle-ci soit alimentée par les données issues des procès-verbaux enregistrés dans des banques de données «de base»: FEEDIS (Feeding Information System) pour la police fédérale et ISLP (Integrated System for the Local Police) pour la police locale. En clair, la majorité des PV que la police rédige est intégrée dans la BNG, au moins de façon partielle.

La police «*connaît*» ainsi pas mal de monde, qui, de manière asymétrique, n'a aucun droit d'accès direct au contenu des informations emmagasinées. Ceci exclut, par conséquent, toute possibilité de débat contradictoire dans l'hypothèse où des policiers décident de tenir compte de ces obscures informations lors de la rédaction d'un procès-verbal, qui, par la suite, peut éventuellement être transmis à un Procureur ou un Juge d'Instruction dans le cadre de poursuites judiciaires. De manière encore plus insidieuse, des informations glanées à votre propos – pouvant inclure vos opinions politiques ou vos tendances religieuses – peuvent potentiellement être prises en compte lors d'une simple visite de l'agent de quartier dans le cadre d'un petit souci de voisinage. Dans le contexte sécuritaire en réponse aux attaques terroristes de Paris et de Bruxelles, la compilation, la conservation, l'utilisation et la communication par l'État de données à caractère personnel dans un fichier de police peut sembler légitime… Mais où placer la limite ?

LA POLICE A VOS DONNÉES. PAS VOUS !

Historiquement, c'est en 1998, suite à l'affaire Dutroux – et des nombreuses critiques qui s'ensuivirent sur les échanges d'informations défaillants –, que la BNG fut créée dans le but d'améliorer la circulation de l'information policière dans le pays. Depuis lors, la BNG rassemble une masse phénoménale de données relatives à des personnes identifiées ou identifiables… mais pas forcément coupables. La ministre de l'Intérieur avait beau tenter de nous assurer en 2013 que « *quand on est dans cette base, ce n'est pas pour des broutilles* »[2], un simple regard sur la loi suffit à convaincre qu'il n'est pas nécessaire d'être un délinquant pour y être enregistré. A titre d'exemple, les services de police ont non seulement l'obligation d'y consigner les données relatives aux personnes condamnées pénalement mais également celles suspectées d'avoir commis une simple infraction administrative. Sont également fichées les personnes «*susceptibles*» de porter atteinte à des biens mobiliers et immobiliers ainsi que les membres de groupements «susceptibles» de troubler l'ordre public. En 2005, la police d'Anvers

(1) Rapport annuel du Comité P 2007-2008.

(2) http://www.lavenir.net/cnt/dmf20131010_00372705.

considérait comme « extrémistes » des organisations comme Gaia, la Ligue Humaniste, Indymedia, l'organisation pacifiste Vaka, le Bond Beter Leefmilieu, le Davidsfonds, le Parti du Travail de Belgique, Médecine Pour le Peuple, le Front Anti-Fasciste, et même Hare Krishna. Étant donné les perquisitions menées en 2014 dans le cadre des «emplois fictifs» dans le cabinet de l'Intérieur de l'Égalité des chances, il ne serait pas étonnant que Joëlle Milquet – pourtant porteuse du projet de réforme de la base de données policière – y soit référencée. En 2015, la Libre Belgique nous informait que les agents de police peuvent enregistrer, dans la BNG, les suspects ou auteurs de délits sous l'appellation «*tzigane*». Moi-même, ayant été candidat aux élections fédérales de 2007 au Parti communiste – erreur de jeunesse – et membre actif de la Ligue des Droits de l'Homme depuis de nombreuses années, j'y suis peut-être inscrit. Qui sait?

De la même manière que pour les adultes, l'inscription en BNG des mineurs âgés de 14 à 18 ans se fait sans l'intervention d'un quelconque magistrat. Aucune limite minimum n'est fixée pour l'inscription en BNG, en contradiction avec les Règles de Beijing et avec la Convention internationale des droits de l'enfant des Nations Unies. Dès lors, un enfant de n'importe quel âge peut être fiché en BNG: les errements de jeunesse sont impardonnables. Clairement, le projet de l'ancien président français N. Sarkozy de fichage dès la crèche est donc d'actualité... Pourtant, la Cour européenne des Droits de l'Homme a estimé que la conservation de données relatives à des personnes non condamnées pouvait être particulièrement préjudiciable dans le cas de mineurs en raison de leur situation spéciale et de l'importance que revêtent leur développement et leur intégration dans la société. Découle de tout ceci d'importants risques d'atteinte à la présomption d'innocence de personnes pourtant reconnues coupables d'aucune infraction. En vertu de la jurisprudence européenne, les suspects et les condamnés doivent pourtant nécessairement faire l'objet d'un traitement différencié. En effet, la Cour européenne est d'avis que si «*la conservation de données privées n'équivaut pas à l'expression de soupçons, encore faut-il que les conditions de cette conservation ne leur donne pas l'impression de ne pas être considérés comme innocents*».

L'objectif de la BNG est évidemment de permettre l'identification des personnes susmentionnées, mais également de croiser ces données avec d'autres informations policières afin de vérifier leurs « *antécédents* » – très subjectifs, puisque non soumis à un contrôle judiciaire – dans le but d'aider les forces de l'ordre dans le cadre de leurs enquêtes et de savoir si des mesures à prendre sont prescrites vis-à-vis de personnes contrôlées (par exemple : fouille, contrôle approfondi, arrestation, saisie, audition, etc.). Les types de données collectées ne sont pas explicitement définies dans la loi et peuvent donc indistinctement consister en des noms, des adresses, des numéros de téléphone, des plaques minéralogiques, des photos, des enregistrements audiovisuels, voire des empreintes digitales ou des traces ADN sans parler des données politiques, syndicales, religieuses ou psychiques... De manière plus générale, peuvent être encodées n'importe quelles informations pour autant que celles-ci présentent un caractère «*adéquat*», «*pertinent*» et «*non-excessif*» pour la poursuite des crimes et délits (mission de police judiciaire) ou la prévention des atteintes à l'ordre public (mission de police administrative).

HASARDEUX ET DURABLE

En première ligne, c'est au policier qui introduit les données dans la BNG auquel revient la responsabilité d'évaluer si celles-ci sont proportionnelles au but poursuivi. A cet égard, il est piquant de relever que des informations fournies par des indicateurs ou par des citoyens déposant plainte – voire de simples rumeurs, dont celles véhiculées par le biais des réseaux sociaux – peuvent tout à fait être encodées dans la BNG dès lors qu'elles sont jugées intéressantes par le fonctionnaire en question. Dans son rapport annuel 2003, le Comité P (organe de contrôle des services de police) indique avoir constaté dans plusieurs dossiers que l'information obtenue est utilisée un peu trop à la légère: « *Dans un cas précis, il s'agissait d'une personne qui aurait été porteuse du virus du sida et aurait eu l'intention de contaminer les fonctionnaires de police lors d'une intervention policière éventuelle. Il est ressorti de l'enquête menée par le Comité Permanent P et par l'Organe de contrôle que l'information enregistrée reposait uniquement sur des rumeurs verbales, qu'il n'y avait aucune justification judiciaire ou administrative, que l'information reçue n'avait pas été évaluée de manière approfondie et qu'il n'y avait pas d'intérêt concret* ».

Outre le degré de qualité hasardeux des données intégrées dans la BNG, une autre préoccupation majeure découle des délais de conservation extrêmement longs prévus par la loi. Globalement, et sauf exceptions, les données relatives aux missions de police administrative sont accessibles aux fonctionnaires durant 5 ans à partir du jour de leur enregistrement et celles relatives aux missions de police judiciaire jusqu'à 15 ans s'il s'agit d'un fait qualifié de délit, 30 en cas de crime. Passé ces délais, ou lorsqu'elles ne sont plus considérées comme étant «*adéquates, pertinentes et non-excessives*», les données traitées en BNG ne sont pas *effacées* mais, au contraire, «*archivées*» pendant 30 ans, tant pour les personnes condamnées que pour celles simplement suspectées. Certes, durant la période « *d'archivage* », les données sont légalement consultables à des fins plus limitatives, il reste néanmoins que le citoyen est en droit de se demander si cette durée de rétention n'est pas contraire au prescrit selon lequel les données doivent être conservées « *pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées* ». Sur base de ce principe, la Cour européenne des Droits de l'Homme n'a d'ailleurs pas hésité à condamner l'État français alors qu'il prévoyait un délai de conservation de 25 ans, inférieur à celui prévu par la loi belge. L'inquiétude de voir les droits à l'oubli et au changement (!) violés est d'autant plus légitime lorsque l'on sait que rien ne prévoit la suppression automatique de données enregistrées dans le cadre d'un fait pour lequel une personne concernée est ensuite acquittée. Une communication vers les services de police est prévue mais, dans l'hypothèse où ceux-ci ne procéderaient pas à l'effacement qui s'impose, aucune voie de recours n'est ouverte aux citoyens. Il existe donc un risque de rester fiché par la police pour une infraction même si on a été acquitté pour ce fait par la justice.

Et ce n'est pas tout : qui dit collecte et enregistrement d'informations parle forcément de communication de celles-ci. Afin d'assurer un partage maximal d'informations, les données figurant dans les banques de données policières peuvent non seulement être consultées par les services de police belges mais également être communiquées à leurs homologues étrangers, aux autorités judiciaires, aux services de renseignements et de sécurité, au comité P, au comité R, à l'OCAM, à la Cellule de traitement des informations financières, à l'Administration générale des douanes et accises, à l'Office des étrangers, aux organisations internationales de coopération judiciaire et policière et aux services de répression internationaux (notamment Europol et Interpol). En outre, nos chers amis peuvent également consulter le Système d'Information Schengen, le SIS. Il a été créé pour compenser la suppression des contrôles aux frontières intérieures de l'espace Schengen.

En principe, ces autorités ne peuvent consulter la BNG que dans le cadre strict de l'exercice de leurs fonctions. Néanmoins, en 2005, le Comité P évoquait déjà « *un certain estompement de la norme* [qui] *régnerait au sein des services de police concernant l'utilisation des applications informatiques mises à leur disposition* ». Pour devoir constater encore dans son rapport annuel 2009 que « *certains membres de la police semblent continuer à abuser de leur accès à des données confidentielles à des fins personnelles* ». Par exemple, selon le quotidien De Morgen, au lendemain du suicide de la chanteuse flamande Yasmine en septembre 2009, plus de 900 policiers auraient consulté ses données. Étant donné la récurrence du phénomène, le Comité P a été amené une nouvelle fois à se pencher sur cette question en 2013 et à diligenter une enquête sur le sujet. Sur cette seule année, 1200 dossiers relatifs à des problèmes quant au respect de la vie privée étaient ouverts au comité P dont 126 comportant spécifiquement des allégations d'utilisation abusive de bases de données. Dans seulement 20,11% des cas, l'examen du dossier permit de conclure au caractère non établi de l'allégation. Dans 77,78% des cas, les faits se situent dans un contexte non professionnel, c'est-à-dire soit purement privé, soit en relation avec le milieu professionnel mais en dehors de l'exécution des missions de police. Paradoxalement, les flics se fliquent eux-mêmes. Les membres des services de police sont effectivement régulièrement l'objet des agissements illégitimes (18,25% des cas) : il s'agit essentiellement des collègues des membres du personnel impliqués. Les autres catégories importantes de victimes sont, par ordre décroissant d'importance : des personnes sans lien direct avec les membres des services de police concernés (14,29%) ; les partenaires, ex-partenaires ou relations de ceux-ci (11,90%) ; et les membres de la famille ou leurs relations (9,52%).

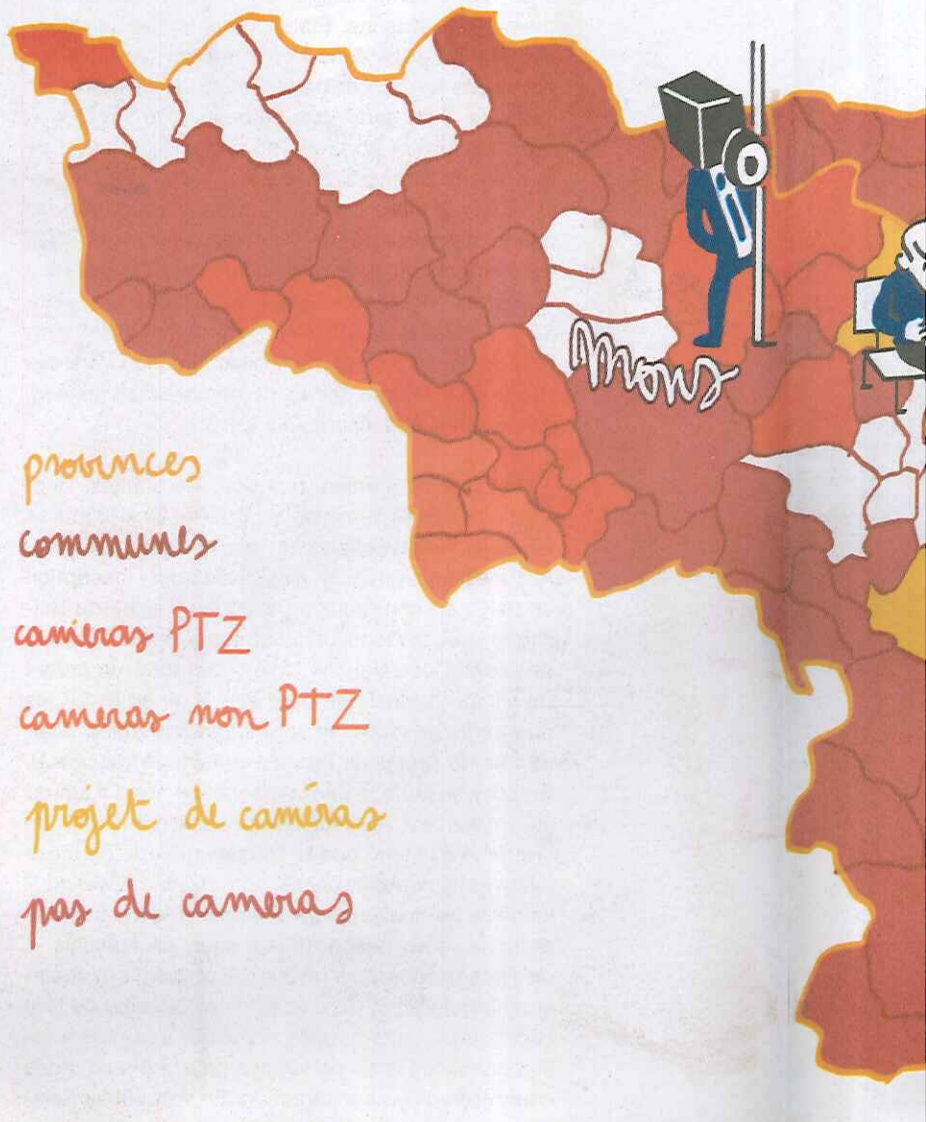
Il est enfin intéressant de relever que la découverte d'accès illégitimes découle davantage de plaintes externes adressées directement aux services de police, à l'AIG ou au Comité P (46,83% des cas) que de plaintes internes à la police (1,59% des cas). Cette information convaincra le lecteur que les chiffres publiés par le Comité P ne sont sans doute que la partie visible de l'iceberg, car pour porter plainte encore faut-il que le citoyen sache qu'il est fiché et que ses données ont été consultées de manière inappropriée... En Belgique, l'accès direct des citoyens aux données dont dispose la police n'est pas permis. Il faut, d'office, passer par l'intermédiaire de la Commission de la protection de la vie privée qui peut opérer ce contrôle, à la demande de la personne visée. C'est ce qu'on appelle le droit d'accès indirect. Pour ce faire, il faut envoyer une demande datée et signée à la Commission. Sous peine d'irrecevabilité, la demande doit contenir : nom, prénom, date de naissance, nationalité de la personne concernée, une photocopie de son document d'identité. Il faut aussi désigner l'autorité ou le service concerné et « *tous les éléments pertinents* ». En réponse, le demandeur n'aura, le plus souvent, pas d'autre information qu'un avis lui signalant que « *les vérifications nécessaires ont été effectuées* ». Il n'y a pas moyen d'être plus opaque.

J'ai bien conscience que cet article n'inspire pas l'espoir de vivre dans une démocratie vivante qui devrait, en principe, débattre de la mise en place d'un dispositif avant de le normaliser, surtout dans le contexte anti-terroriste actuel. Et j'en rajoute, malheureusement, en guise de conclusion: la BNG est régulée par voie législative seulement depuis mars 2014. Avant cette date, la BNG n'était encadrée que par le biais de circulaires ministérielles et de directives internes non consultables par le citoyen. Mais depuis lors, les statistiques relatives à son contenu sont inexistantes: la loi qui avait pour objet de rendre la BNG transparente a produit le résultat inverse. La Ligue des Droits de l'Homme et la Liga voor Mensenrechten ont décidé d'introduire un recours devant la Cour constitutionnelle contre la nouvelle loi sur la gestion de l'information policière. Croisons les doigts.

Franck Dumortier

CAMÉRAS INTELLIGENTES:

PRÉVENTION, STRATÉGIE POLITIQUE OU SURVEILLANCE GÉNÉRALISÉE DE L'ESPACE PUBLIC ?



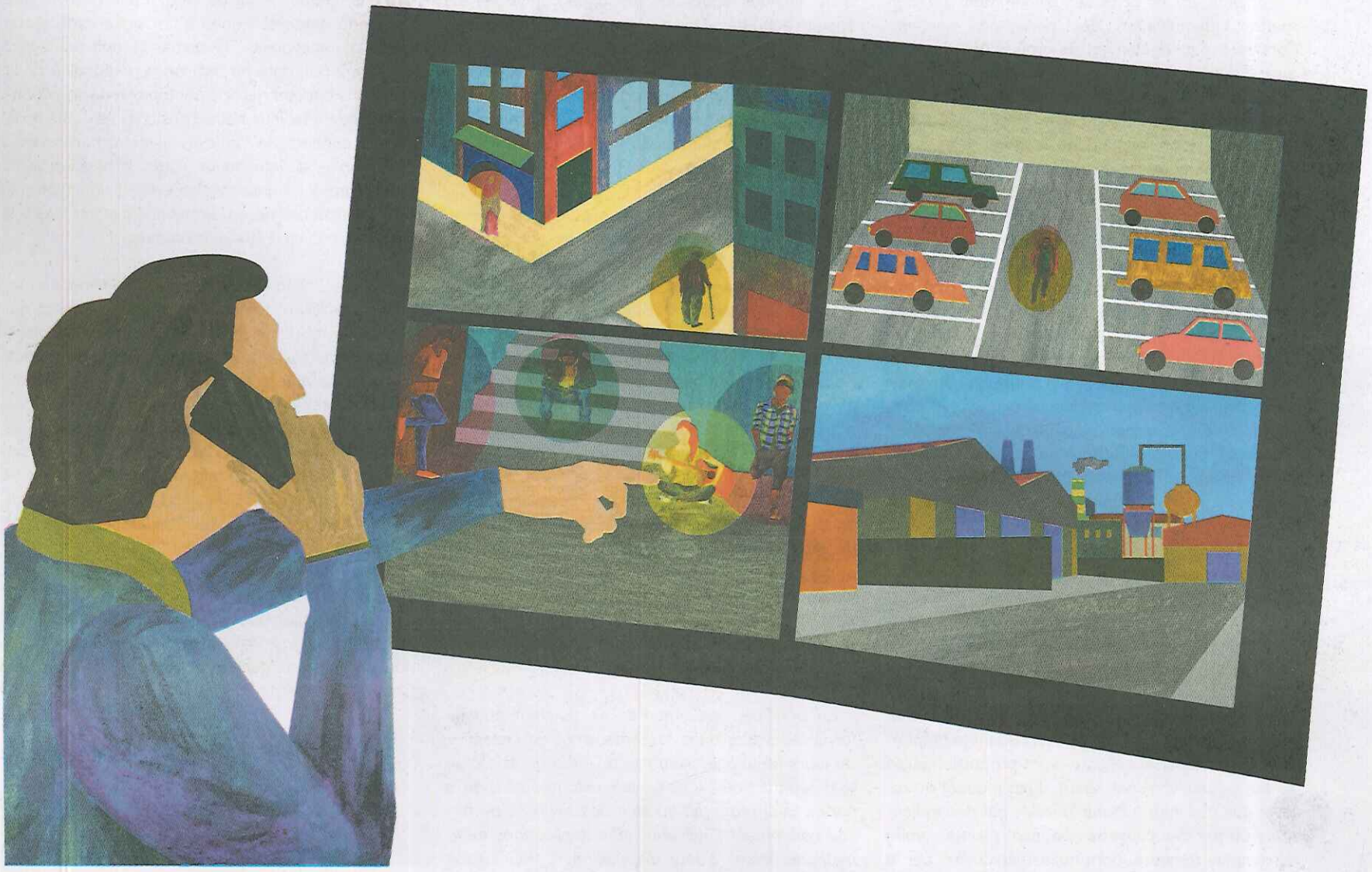


Illustration: Teresa Arroyo Corcobado

Depuis une vingtaine d'années, les caméras de surveillance fleurissent dans nos villes. Pourtant, peu d'informations circulent sur les raisons de leur installation à tel ou tel endroit, sur leur efficacité réelle, sur leur nombre, sur leurs emplacements, sur le traitement des images, sur nos droits en tant que citoyens.

Néanmoins, nos politiques publiques financent la vidéosurveillance, et nos ingénieurs travaillent à rendre les caméras de plus en plus intelligentes, plus autonomes, c'est-à-dire capables d'identifier sans l'aide de l'humain des comportements considérés comme "suspects". Si ces développements peuvent représenter un défi technique stimulant, ils posent néanmoins de nombreuses questions éthiques et juridiques.

UNE ÉTUDE QUALITATIVE DE L'UTILITÉ DES CAMÉRAS PTZ EN WALLONIE[1]

Les caméras PTZ (présentes dans nos espaces publics wallons) sont capables de zoomer en direct à plus de 300 mètres et de filmer des vues panoramiques à 360 degrés, tant sur l'axe horizontal que vertical. Elles sont programmables pour zoomer sur une zone spécifique, ou pour détecter des mouvements et suivre l'objet ou la personne détectée (e.g. *auto-tracking* d'un engin ou d'une personne dans une zone à risque). Elles parviennent également à détecter un mouvement inhabituel d'un point A à un point B (e.g. une voiture en sens interdit). Mais la technologie PTZ n'est pas encore tout à fait au point. Il arrive par exemple qu'une caméra reste coincée sur l'image d'un drapeau qui flotte à cause du vent car la caméra a «intelligemment» détecté un mouvement…

Le défi technique est donc de développer des algorithmes de traitement d'images capables de «*détecter de manière automatique et en temps réel des cibles potentiellement "suspectes" ou "anormales"*[2]. L'intelligence de ces dispositifs permettrait d'éviter le visionnage des images par des opérateurs. Mais de tels développements techniques ont des implications sur la gestion politique des espaces urbains, sur l'organisation du travail et sur la question du vivre-ensemble dans les villes. Le danger réside également dans le côté arbitraire des critères définissant un comportement suspect et les dérives potentielles qui en découlent (typiquement si les critères devenaient, demain, la couleur de peau, le port de la barbe ou de la burqa).

CONSTATS : EFFICACITÉ RELATIVE ET INADÉQUATION AVEC LES ATTENTES

Notre recherche a porté sur l'analyse approfondie de l'utilité intrinsèque de la vidéosurveillance en milieu urbain, dans les espaces publics ouverts – rues, parkings publics, places, entrées et sorties de zonings industriels. Pour cela, nous avons d'abord procédé à un recensement inédit des caméras de surveillance en Région wallonne (voir carte ci-contre) Il en ressort que 20% des communes sont équipées de caméras, et parmi elles, 15% ont investi dans la technologie PTZ. Nous avons ensuite rencontré des acteurs clés (chefs de corps, porteurs de projets de vidéosurveillance[3], utilisateurs du dispositif dans leur travail quotidien) de vingt communes wallonnes équipées de caméras PTZ, pour comprendre les tenants et aboutissants de l'implémentation de la vidéosurveillance. Enfin, nous avons organisé des débats avec des citoyens aux profils variés, afin de confronter les discours du terrain à ceux de la société civile.

L'analyse croisée de ces résultats nous permet de montrer, en contexte urbain, le manque d'adéquation des caméras intelligentes avec les attentes concrètes du terrain et les priorités des citoyens, ainsi que leur coût élevé (coût financier[4] et humain). On attribue aux caméras un pouvoir qui s'avère plutôt symbolique et politique que démocratique.

À la question «*Pour quelles raisons des caméras ont-elles été installées dans votre commune ?*», les acteurs rencontrés parlent avant tout d'un objectif de prévention et de maintien de l'ordre public: volonté de rassurer les citoyens, créer un sentiment de sécurité et de tranquillité, dissuader les criminels. Peu de communes réalisent cependant une analyse des besoins pour cibler les endroits à surveiller par caméras… Derrière cet objectif «préventif» se manifeste en fait une volonté politique de poser des actes *symboliques* forts en faveur d'une tranquillité urbaine.

En outre, nos entretiens ont révélé une volonté de lutter, grâce aux caméras, contre les petites incivilités: bagarres, graffitis, dépôts d'ordures, déjections canines, trafic de cannabis, rassemblement de jeunes[5]. Ces incivilités sont source d'insécurité, selon nos informateurs et les citoyens. Mais concrètement, les caméras sont-elles utiles pour résoudre ce problème? L'effet dissuasif semble moindre dans les grandes villes. Dans les plus petites villes, on observe plutôt un *déplacement* des actes délictueux en présence de caméras. Il est certes positif de montrer l'image d'un centre-ville propre et sécurisé, mais qu'en est-il si cela est fait au détriment des périphéries urbaines? Et si cela crée des quartiers de relégation de la saleté et de la petite criminalité? En outre, même si la caméra a un pouvoir rassurant pour certains, elle a aussi un pouvoir stigmatisant pour d'autres… Ajoutons à cela le constat selon lequel les caméras n'ont aucun effet dissuasif sur les délits spontanés et impulsifs, surtout si ces délits ont lieu dans des endroits bondés ou festifs.

Certains informateurs pensent que les caméras auraient un réel effet dissuasif s'il y avait un mode de répression directe sur base des images… Ceci nous amène à un autre constat de notre enquête: il faut des humains pour visionner les images en temps réel, et cela a un coût. Par conséquent, rares sont les communes où des opérateurs assurent une permanence de visionnage – exception faite de quelques grandes villes. Lorsque les images sont visionnées en direct, c'est généralement en parallèle à de nombreuses tâches… Or, il ressort de notre enquête que les caméras sont réellement utiles en cas d'utilisation proactive. Nombreuses villes en ont fait l'expérience lors d'événements ponctuels (carnaval, festival, marché de Noël, match de foot…): les policiers consultent les images en direct et guident les patrouilles sur le terrain plus efficacement. Les caméras peuvent également être utilisées de façon proactive pour réguler la circulation en direct, pour fluidifier le trafic et assurer la sécurité routière.

Il apparaît donc que les caméras constituent une réelle plus-value au travail des policiers dans certaines situations, mais qu'elles ne remplaceront jamais les hommes de terrain, selon les personnes interrogées. En outre, un problème majeur se manifeste: le déploiement de caméras de surveillance est souvent réduit à un investissement purement technique, qui ne prend pas en compte l'influence de ce nouvel «acteur» dans l'organisation humaine du travail. Cela entraîne des difficultés d'appropriation par les opérateurs, car leurs tâches quotidiennes n'ont pas été adaptées à l'arrivée des caméras.

Un autre argument employé pour justifier l'implémentation de caméras est la récolte d'un *matériel de preuve objectif*. Les images sont supposées apporter un élément «neutre» pour mieux comprendre une scène/un comportement. Mais cette utilisation de la caméra doit être nuancée. D'une part, parce que les controverses juridiques sont nombreuses quant à la loi applicable en matière de collecte d'images à des fins de preuves[6]. D'autre part, parce qu'il n'existe pas de chiffres permettant d'établir un lien probant entre l'installation de caméras et la diminution du taux de criminalité ou l'augmentation du sentiment de sécurité. Les communes ne réalisent pas de rapports pour évaluer l'impact des caméras. Par contre, quelques communes calculent le nombre de fois où les images ont été utiles dans le cadre d'enquêtes judiciaires. Par «utiles» il faut entendre que les images ont apporté un *élément* complémentaire (une date, une heure, un profil du suspect, une description précise de la scène d'un accident etc.) et non de clôturer définitivement l'enquête, en aidant à attraper le responsable d'un délit ou en disculpant un coupable potentiel. Les quelques chiffres récoltés par les communes nous permettent de dire que les images aident dans 20 % des cas à avancer dans une investigation, mais cela requiert un travail de visionnage fastidieux pour retrouver *la* bonne image. Il s'agit d'un choix politique d'investir dans un système de vidéosurveillance coûteux dont l'utilité peut sembler moindre….

Il est primordial pour nos politiques d'envisager d'autres options, en parallèle. Dans cette optique, nous nous sommes penchés en profondeur sur l'argument du sentiment d'insécurité employé pour justifier la vidéosurveillance dans nos villes. Il ressort du discours des citoyens que le sentiment d'insécurité est moindre dans les petites et moyennes villes, et un peu plus élevé dans les grandes villes. Plus intéressant encore, la grande majorité des personnes rencontrées perçoit le sentiment d'insécurité comme une problématique globale, multifactorielle. Les éléments les plus cités pour parler de lutte contre l'insécurité sont l'éclairage des rues, la propreté, la cohésion sociale et la réduction des inégalités sociales. Les citoyens posent la question de la sécurité de manière large, en termes socio-économiques et de «bien-être en ville». Ils placent ainsi au cœur du débat les *enjeux* démocratiques liés à la vidéosurveillance. Selon eux, si l'espace public est un territoire partagé et collectif, la sécurité et les dispositifs sécuritaires attachés devraient également être gérés de manière collective, et non de manière top-down.

À l'ère de la lutte contre le terrorisme, des polémiques liées à l'afflux de migrants, la question de l'utilité de la surveillance urbaine doit impérativement être débattue démocratiquement dans notre société. La rhétorique sécuritaire est récurrente dans les discours politiques et médiatiques, permettant ainsi de justifier une surveillance –presque paranoïaque – de tous les citoyens, et une présence militaire dans nos rues… Cette surveillance généralisée illustre notre volonté actuelle de contrôler tous les pans de la société, de nos vies. Mais le contrôle absolu n'existe pas, et la sécurité absolue est un leurre… À force de vouloir tout contrôler, nous créons de nouvelles failles au système que nous cherchons à protéger. Posons-nous donc la question du sens des moyens de contrôle et de surveillance mis en place dans nos sociétés, de leur impact réel, et de la confiance que nous accordons à des objets technologiques. Demandons-nous où l'argent public devrait-il être prioritairement investi: dans l'aménagement du territoire, dans les associations locales présentes sur le terrain, dans la présence policière, dans la vidéosurveillance? Au vu de la multiplication des politiques d'austérité qui nous touchent, nous sommes en droit, comme citoyens, de nous demander si la vidéosurveillance vaut la peine.

Perrine Vanmeerbeek,
Unité Technologie et Société, CRIDS

(1) Les données empiriques qui servent de base à cet article ont été récoltées entre 2013 et 2015, dans le cadre d'un projet de recherche appliquée financé par les fonds GreenTIC de la Région wallonne. Le projet rassemblait un consortium constitué d'ingénieurs, d'informaticiens, et de membres du Centre de Recherche en Information, Droit et Société (CRIDS, Université de Namur). La recherche portait sur les caméras PTZ (Panoramic-Tilt-Zoom).

(2) L'équipe technique du projet a défini quatre types de comportements "suspects" que les caméras intelligentes sont censées détecter: des voitures à contre-sens, une personne qui court, une personne qui maraude, un groupe de plus de quatre personnes.

(3) Notons que la décision d'installer ou non des caméras de surveillance revient au *bourgmestre*. Or, ce sont les policiers qui *utilisent* les caméras: ils sont les seuls autorisés à visionner les images. On observe donc un décalage entre les *décideurs* et les *utilisateurs* de la vidéosurveillance urbaine.

(4) Prix d'une caméra PTZ: minimum 5000 €. Coût global d'installation d'une caméra PTZ (comprenant le coût de l'acheminement des images par fibre optique): entre 12000 € et 38000 € selon les villes, selon l'endroit où l'on installe la caméra. Certaines communes louent la bande passante à des sociétés privées (Belgacom, SNCB). Prix d'une caméra ANPR (qui photographie les plaques de voitures): environ 15000 €. Prix d'une caméra fixe: environ 1000 €. A ces coûts d'installation s'ajoutent les coûts d'entretien et de maintenance du réseau de vidéosurveillance (exemple pour une grande ville: 100000 €/an).

(5) Nos informateurs considèrent souvent «les jeunes» comme source d'insécurité. Ce constat n'est pas le propos de cet article, mais il mériterait d'être approfondi.

(6) À ce sujet, voir l'article de Franck Dumortier (2013), Franck Dumortier (2013), «La surveillance par caméras: de la supervision de lieux vers l'observation systématique de personnes», in : *Discipline et surveillance dans la relation de travail*, 333-342, Anthemis.

SURVEILLANCE DE MASSE : ENTRE SURVEILLANCE COMMERCIALE ET SURVEILLANCE RÉPRESSIVE

L'éventail de mesures de traitement de données à caractère personnel à grande échelle est multiple et ne cesse de se développer. Ainsi, récemment, le gouvernement se targuait d'adopter des nouvelles mesures visant à lutter contre le terrorisme dont le *Passenger Name Record* (PNR), qui suppose la création d'une base de données à partir des informations fournies par les sociétés de transport. Dans un autre registre, la rétention de données oblige les entreprises à collecter et stocker les métadonnées de l'ensemble des utilisateurs de réseaux de communications. Si l'arsenal s'étoffe, les autorités font fréquemment appel aux acteurs privés pour obtenir certaines informations. En effet, à l'heure du *big data*, la quantité de données traitées par des sociétés commerciales est exponentielle d'autant qu'elle constitue un enjeu financier notable. La surveillance de masse n'est donc pas qu'une simple affaire de «nouvelles mesures» censées apporter du grain à moudre aux enquêteurs, une surveillance basée sur la collaboration entre autorités publiques et acteurs privés est tout aussi intrusive.

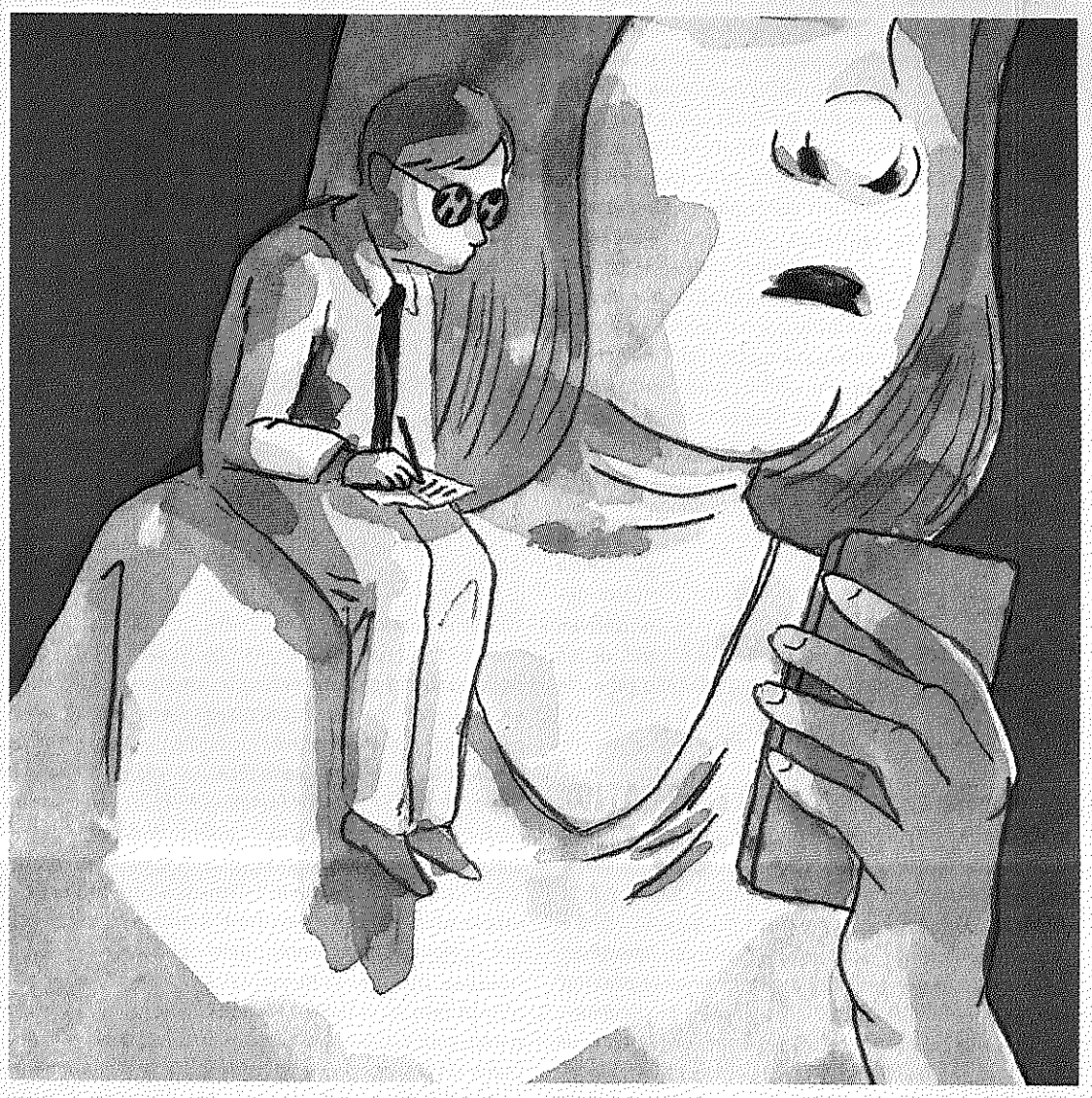


Illustration : Aurore Vegas

UNE AIGUILLE QUI NE CESSE DE SE PERDRE DANS LA BOTTE DE FOIN

La polémique relative au traitement de données à grande échelle occupe une partie de la scène médiatique depuis les révélations du lanceur d'alerte Edward Snowden, en juin 2013, lorsque ce dernier met en lumière les programmes de la National Security Agency (NSA) au moyen desquels les États-Unis interceptent au niveau mondial le contenu de nos communications. Ces données, collectées secrètement , sont susceptibles d'être transmises à des services de renseignements étrangers. En Belgique, par exemple, les services de renseignements peuvent utiliser des informations recueillies par la NSA sans être tenus de chercher à savoir si les données ont été collectées légalement[1].

Au niveau européen, le débat du traitement de données à grande échelle fut alimenté par l'implémentation d'une directive européenne relative à la rétention de données. Cette mesure impose aux opérateurs de télécommunications de collecter et de stocker l'ensemble des métadonnées: adresse IP, pseudonymes utilisés, listes de contacts, dates et heures d'envoi et de réception des courriers électroniques, sites internets consultés, dates et heures de connexion, etc. Les métadonnées, qui ne prennent pas en considération le contenu des communications ou des courriers électroniques, doivent être stockées durant une certaine période pour être accessibles (sur demande) aux autorités répressives. La rétention de données et le stockage de celles-ci s'opèrent donc *a priori*, de manière systématique et indifférenciée, indépendamment de l'ouverture d'une enquête pénale; l'accès aux données collectées par les autorités répressives suppose par contre l'existence d'une telle enquête.

La directive «*rétention de données*», une fois transposée en droit belge, fut directement portée devant la Cour constitutionnelle. Ses détracteurs invoquaient le caractère disproportionné d'une telle mesure vu la gravité de l'atteinte au droit à la vie privée. Ils soulignaient également le risque de stigmatisation de personnes présumées innocentes mais potentiellement suspectes, les données de l'ensemble des utilisateurs étant collectées sans aucun lien avec l'ouverture d'une enquête pénale. Le 8 avril 2014 - au niveau européen -, le 2 juin 2015 - au niveau belge -, la Cour de Justice de l'Union européenne et la Cour constitutionnelle ont invalidé et annulé les dispositions en cause. Les juges pointent l'absence de garanties suffisantes prévues par la mesure au regard de l'étendue des données collectées. La Cour constitutionnelle reprenant les termes de la Cour de Justice, relève en outre: «*La circonstance que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées* [...] *le sentiment que leur vie privée fait l'objet d'une surveillance constante*».[2] En effet, la rétention de données, même si elle ne concerne pas le contenu de nos communications, reste très intrusive dans la mesure où les métadonnées « *prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées* »[3]. Tant les juges européens que belges ont donc mis un (premier) frein au stockage massif et indifférencié des métadonnées. Leurs décisions imposent au législateur de revoir les dispositions afin de limiter l'atteinte à la vie privée au strict nécessaire, par exemple en prévoyant une durée de conservation de données plus courte. Premier frein étant donné qu'à l'heure où nous écrivons ces lignes, la Belgique est en passe d'adopter une nouvelle loi. Le sujet est donc loin d'être clos d'autant que la disposition adoptée dans la foulée des attentats de Londres et de Madrid en 2005 au niveau européen, n'a fait l'objet d'aucune étude suffisamment concrète permettant d'affirmer qu'elle est efficace à des fins de lutte contre la grande criminalité et le terrorisme.

Enfin, plus discrètement, le gouvernement s'apprête à se doter d'un *Passenger Name Record*, soit de prévoir un traitement de données des passagers. Le PNR à la belge vise à élaborer une base de données à partir des informations fournies par les usagers des compagnies aériennes, de trains et bateaux internationaux. Ce fichier national supervisé par le Service Public Fédéral Intérieur a la particularité d'être soumis à un algorithme particulier croisant certaines données afin d'établir des profils particuliers en vue de déceler les éventuels terroristes, mais aussi de lutter contre l'immigration illégale. A l'instar de la rétention de données, cette base de données est consolidée a priori, indépendamment de l'ouverture d'une enquête pénale, mais implique également un traitement de données à des fins de profilage. Cette mesure particulièrement critiquée pour son caractère «préventif», laisse également en suspens la question de l'efficacité du PNR pour at-

(1) A ce sujet, voir le rapport annuel du Comité R disponible à l'adresse suivante : http://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2014.pdf

(2) C.J.U.E., 8 avril 2014, Digital Rights Ireland Ltd & Michael Seitlinger e.a., affaires jointes C-293/12 & C-594/12. 8 avril 2014. Point 37 et 65 C.C., 11 juin 2015, n°84/2015.

(3) Points 26-27 et 37 de l'arrêt Digital Rights.

teindre l'objectif poursuivi. A titre illustratif, les déplacements par véhicules motorisés comme ce fut le cas pour les attentats de Paris ne sont pas détectés, les bombes pourront toujours exploser aux entrées des aéroports comme ce fut le cas pour les attentats de Bruxelles, par exemple. De plus, en pleine lutte contre la fraude sociale voire en pleine lutte contre les assurés sociaux, face à cette manne d'informations, le risque de détournement de la finalité initiale est alléchante.

Les techniques de traitement de données à grande échelle mises en place par les autorités, sont donc surtout critiquées pour leur absence de proportionnalité considérant que «*la surveillance de masse a des répercussions potentiellement graves sur la liberté de la presse, la liberté de pensée et la liberté d'expression, ainsi que sur la liberté de réunion et d'association, et qu'elle entraîne un risque élevé d'utilisation abusive des informations collectées à l'encontre d'adversaires politiques*»[4]. Or, pour être conforme à la Convention européenne des Droits de l'Homme, une ingérence doit être nécessaire et proportionnée. Le législateur, avant l'adoption d'une disposition, est censé s'assurer qu'il n'existe pas d'autres mesures moins contraignantes ou permettant déjà d'atteindre le but poursuivi. En l'occurrence, outre l'absence de démonstration claire et avérée de l'efficacité d'un stockage massif et indifférencié de données à des fins de lutte contre le terrorisme, la nécessité de mettre en place de tels dispositifs peut également être mise en cause.

Illustration : Aurore Vegas

UN DÉPLACEMENT DE LA SURVEILLANCE VERS LES ACTEURS PRIVÉS

Les acteurs privés sont considérés comme des intervenants privilégiés dans le cadre d'enquêtes pénales dans la mesure, en traitant des données à des fins de marketing et de facturation, ils accèdent automatiquement à un ensemble de données à caractère personnel. Ces données une fois collectées, peuvent être stockées pendant une certaine période pour être soumises à des algorithmes particuliers. Sur Internet par exemple, nombres de services gratuits type Skype, Facebook, Google, Twitter, Youtube, Amazon... traitent nos données numériques «en masse» afin d'établir des profils de consommation. Le flux de données entre les acteurs privés et les autorités répressives est fréquent. En effet, en Belgique, les acteurs privés sont expressément tributaires d'une obligation de collaboration envers les autorités judiciaires; ils prêtent dès lors régulièrement leur concours dans le cadre d'enquêtes pénales. Un procureur peut solliciter auprès de fournisseurs d'accès à Internet semblables à VOO, Proximus, Telenet, certaines données de communications à savoir l'identité de l'abonné d'une ligne téléphonique, d'une adresse de courrier électronique, d'une connexion internet, d'une adresse IP, etc. Un juge d'instruction pourra croiser ces données pour, par exemple, géolocaliser une personne, identifier ses déplacements, intercepter ses communications ou intercepter ses courriers électroniques. Dans certains cas, ce dernier pourra également forcer les personnes présumées disposer d'une connaissance particulière d'un système informatique, à collaborer en bloquant l'accès aux données ou en fournissant la clé de chiffrement si les données sont cryptées. La personne sollicitée a la possibilité de se réfugier derrière le droit au silence, à condition d'être directement impliquée dans l'enquête. Enfin, certains intermédiaires et notamment les hébergeurs de sites internet, sont tenus de dénoncer au procureur du Roi les activités ou informations illicites dont ils auraient connaissance. Ils doivent également bloquer sur demande ou de leur propre initiative les sites «*incitant à la haine*» par exemple, ou faisant «*l'apologie du terrorisme*».

Si la plupart des sociétés se « prêtent au jeu », certaines refusent parfois de collaborer. Ainsi, Yahoo! a déjà contesté la demande d'un procureur lui imposant de communiquer certaines données. Le Parquet souhaitait déterminer l'identité de plusieurs utilisateurs d'adresses électroniques utilisées dans le cadre d'une affaire d'escroquerie. Néanmoins, Yahoo! ne voulait pas donner suite à la demande. La société motivait son refus en invoquant l'absence d'autorité de la loi belge à l'égard d'une entreprise américaine soumise au droit américain. De plus, elle contestait être tenue d'une obligation de collaboration puisque la demande émanait d'un procureur et non d'un juge d'instruction. En effet, le juge d'instruction peut faire intervenir l'ensemble des acteurs privés ou presque, alors que le Parquet devait se limiter, en principe, aux fournisseurs d'accès à Internet, c'est-à-dire par exemple VOO ou Proximus. La Cour de cassation a finalement tranché la controverse. Elle considère en premier lieu que la loi est applicable à toute entreprise «*qui fournit des mails en Belgique, participe à la vie économique (du pays)*». En second lieu, selon la Cour, l'obligation de fournir certaines données et de collaborer à la demande du procureur ne se limite pas aux fournisseurs d'accès à Internet tels que l'invoquait 'Yahoo!' mais s'étend à tout acteur offrant des services de communications électroniques. La nuance est importante puisque par cette interprétation, le juge permet au procureur d'obtenir des données auprès de la plupart des services disponibles sur Internet tels Skype ou Facebook, sans devoir faire appel au juge d'instruction. Or, l'ouverture d'une instruction est censée offrir à la personne inculpée l'apport de certaines garanties contre le risque d'accès illicites et arbitraires aux données.

Dans la même logique, récemment, la société Apple a refusé d'obtempérer à une injonction du FBI lui ordonnant de déchiffrer le téléphone portable d'un des auteurs de la tuerie de San Bernardino. Outre le déblocage du téléphone, le FBI souhaitait qu'Apple élabore une nouvelle version du système d'exploitation. Cette assistance technique aurait permis aux services répressifs américains de faciliter le déverrouillage de n'importe quel smartphone. Or, selon Apple, un tel logiciel facilitant l'accès aux téléphones met à mal la sécurité et la confidentialité des données stockées. En bout de course, le FBI finit par trouver une faille lui permettant d'accéder aux données contenues sur le téléphone. *In casu*, les services d'enquêtes américains vont plus loin que la «simple» obligation de collaboration exposée ci-avant. Les enquêteurs souhaitaient en effet forcer un acteur privé à concevoir des portes facilitant l'accès aux données contenues. En Belgique, une telle obligation n'existe pas mais pourrait se concevoir. Actuellement, la loi autorise par contre les services de renseignement à pirater un système informatique « *à l'aide ou non de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités* ». Ces derniers sont donc en mesure de s'immiscer dans un ordinateur en insérant un virus informatique par exemple et de collecter les informations souhaitées. Celles-ci pourront être transférées aux services de police si cela s'avère nécessaire.

En conséquence, si le traitement de données à grande échelle à travers des mesures telles l'obligation de rétention de données ou l'accord PNR fait couler beaucoup d'encre pour des raisons de proportionnalité, force est de constater que, outre l'absence d'efficacité démontrée *in concreto*, le caractère «nécessaire» de tels dispositifs pourrait également susciter un large débat. Les données des voyageurs collectées par les agences de voyage par exemple, sont déjà accessibles sur demande du procureur du Roi. De même, le Parquet a la possibilité d'accéder aux données de communications déjà conservées par les opérateurs à des fins commerciales indépendamment donc de l'existence d'une obligation de rétention. Sans parler du coût de telles mesures, le débat relatif à la surveillance de masse devrait donc être élargi. En effet, la frontière entre surveillance «de masse» commerciale et surveillance «de masse» sécuritaire est loin d'être étanche. Dès lors, un cryptage généralisé reste la réponse la plus efficace pour protéger notre vie privée.

Catherine Forget

(4) Ibid., point 10.

COMMENT DÉJOUER LES DISPOSITIFS DE SURVEILLANCE ?

RUSES ET TACTIQUES DE RÉSISTANCE DANS LES ENVIRONNEMENTS NUMÉRIQUES

Face à l'émergence spectaculaire de technologies de plus en plus intrusives capables de collecter, d'analyser, de traiter des quantités gigantesques de données à des fins de profilage et de surveillance, les citoyens se trouvent de plus en plus démunis. Comment faire pour échapper au traçage permanent dans un contexte où les dispositifs techniques facilitent l'exploitation de données à l'insu des personnes ? Est-il réaliste d'attendre des citoyens qu'ils «gèrent» leurs données et assurent un contrôle sur leurs profils alors qu'ils manquent très souvent de la plus élémentaire familiarité avec les technologies qu'ils utilisent ?

Les débats contemporains autour de la vie privée et des données dites «personnelles» opposent à leurs extrêmes deux conceptions totalement contradictoires du pouvoir de l'individu à l'ère de la nouvelle «*gouvernementalité algorithmique*»[1] : ils consacrent, d'un côté, le fantasme d'un pouvoir absolu de l'individu autonome et responsable sur ses données ; de l'autre, le cauchemar d'une hétéronomie totale d'un individu passif et impuissant. Représentant les deux faces d'une même médaille, ces conceptions négligent de prendre en compte l'émergence progressive d'une variété de formes quotidiennes de résistance qui se déclinent à travers la mise en scène d'actions modestes, minuscules et fragmentaires[2]. Parmi les formes subtiles de contrôle situées dans cette zone grise entre autonomie et hétéronomie totale, il est en effet possible d'identifier une série de pratiques subversives procédant de ce qu'on appelle communément la ruse. Conscients des limites inhérentes aux processus de réglementation ou d'autorégulation pour répondre aux risques soulevés par la prolifération des mécanismes de profilage dans les environnements numériques, différents acteurs se sont organisés de manière plus ou moins formelle et ont développé ces dernières années un ensemble de projets destinés à déjouer ces mécanismes, à retourner l'arme de l'ennemi contre lui-même et à «traquer les traqueurs».

Ces projets visent à concevoir et diffuser sur Internet des outils techniques permettant à la fois d'informer les utilisateurs et de leur donner l'opportunité de résister aux mécanismes de profilage et de surveillance grâce à différents subterfuges. D'un point de vue technique, ces projets se manifestent généralement par leur grande simplicité. Ils ne s'appuient pas, ou que très rarement, sur le développement d'architectures techniques lourdes et complexes, comme les procédés de cryptographie. En outre, ils mettent à disposition des utilisateurs des logiciels ou des applications non seulement faciles d'usage, mais qui en plus ne nuisent pas au bon fonctionnement de leur machine. Ensuite, les outils mis à la disposition des utilisateurs par ces projets diffèrent dans leurs effets d'autres tactiques bien connues visant à garantir le secret ou l'anonymat. On pense par exemple à l'usage de plates-formes anonymes comme Tor[3]. Pour les protagonistes de la ruse, la disparition, le secret, l'anonymat ou le refus total ne sont pas vraiment des options. A celles-ci, ils préfèrent l'intelligence pratique et l'art de la tromperie.

La ruse est une notion faisant généralement référence à l'ingéniosité, l'inventivité et la créativité déployée dans des usages quotidiens. A ce titre, cette notion entretient un lien fort avec l'habileté, les gestes, les routines et les savoir-faire requis notamment pour développer et manipuler les objets techniques et les machines. Dans la littérature dédiée aux usages des médias ou des technologies de l'information et de la communication, cet «art du truc» ou du bricolage a été largement commenté pour décrire, par exemple, la virtuosité technique des développeurs de logiciels libres ou des pirates informatiques. Les développeurs participant aux projets que nous évoquons ici témoignent assurément des mêmes qualités. L'intelligence pratique caractérisant la *ruse* se décline ici à travers un premier mouvement tactique consistant, grâce à un procès de familiarisation avec les mécanismes de traçage et de profilage, à «trouver le truc» qui va permettre d'en exploiter les failles[4]. Il s'agit alors prioritairement d'ouvrir les «boîtes noires» algorithmiques, grâce à des procédés de rétroingénierie, pour en comprendre les rouages. Un tel rapport familier aux objets est justement ce qui fait très souvent défaut aux «utilisateurs ordinaires» dont les capacités et compétences semblent plus que limitées lorsqu'il s'agit d'une part de manipuler leurs machines, d'autre part de protéger leurs données. Dans leurs rapports quotidiens aux environnements et aux dispositifs numériques, la plupart des individus ordinaires s'engagent dans des routines maladroites, voire contradictoires, qui ne leur offrent pas de prises sur leurs données et peuvent s'avérer dangereuses. C'est ce que les différents protagonistes de ces projets s'efforcent de compenser en mettant à la fois leur virtuosité et leurs astuces au service des utilisateurs profanes.

L'intelligence pratique propre à la ruse se déploie alors à travers un second mouvement prenant la forme d'une «pédagogie de la ruse». Une fois les boîtes noires des mécanismes de traçage et de profilage *dé-faites*, on en dévoile le fonctionnement aux utilisateurs ordinaires. Dans cette perspective, ces différents projets ont pour ambition d'informer les utilisateurs et de mettre à leur disposition divers instruments (tels que des bases de données de cookies, des cartographies de traces, des systèmes d'évaluation des entreprises, etc.) permettant de mieux comprendre l'utilisation qui est faite de leurs données par les réseaux publicitaires, les fournisseurs de données comportementales, les éditeurs de sites web et autres sociétés qui s'intéressent à leur activités en ligne. Il s'agit en quelque sorte de promouvoir une éthique du *Do it Yourself* en révélant aux utilisateurs ordinaires trucs et ficelles afin de rendre leur expérience dans les environnements numériques plus sensée.

Au-delà de leurs vertus pédagogiques, n'oublions pas que ces différentes tactiques de résistance servent avant tout à tromper. Tel est le propre de la ruse. Or si celle-ci a pour objectif de jouer un (mauvais) *tour*, il faut avoir à l'esprit que les effets recherchés ainsi que les moyens peuvent varier. En effet, plusieurs artifices/artéfacts peuvent être utilisés pour différents types de mystifications.

Par exemple, certains de ces projets ont recours à ce que Brunton et Nissenbaum appellent l' «obfuscation» et qu'on peut définir comme la production et la communication de données trompeuses, ambiguës ou fausses dans le but de susciter la confusion et de rendre la collecte de données moins fiable et donc moins précieuse pour les agrégateurs de données[5]. Le projet TrackMeNot (TMN), notamment, propose une extension de navigateur (*browser extension*) ayant pour objectif de prévenir, ou du moins de limiter, le profilage exercé à travers les moteurs de recherches. Au lieu de recourir à des outils cryptographiques afin de couvrir les traces, TrackMeNot masque les requêtes des utilisateurs en s'appuyant paradoxalement sur la stratégie inverse : le bruit et l'obfuscation. Avec TMN, les requêtes réelles des utilisateurs sont cachées au milieu de recherches fantômes générées par le système et lancées sur les moteurs que les utilisateurs choisissent. En d'autres termes, TMN masque les recherches des utilisateurs dans une nébuleuse de fausses recherches afin de compliquer le profilage des utilisateurs et de le rendre inefficace. Dans le même ordre d'idées, le projet bien nommé Ad Nauseam clique automatiquement sur toute publicité préalablement bloquée et, ce faisant, enregistre une visite pour l'annonce concernée au sein des bases de données des réseaux publicitaires. Ce flux de clicks omnivore et ininterrompu révèle une absence totale de logique, rendant ainsi les données collectées inutilisables à des fins de profilage, de ciblage ou de surveillance. En simulant le comportement d'un utilisateur sans déguiser son identité et sans rendre ses données comme telles illisibles, ces logiciels visent à brouiller son profil en le «cachant dans la foule», en le noyant dans la masse.

D'autres projets développent des outils basés sur un modèle de ruse différent. Ils visent notamment à travestir l'identité des utilisateurs sur les réseaux sociaux. Le projet Undefined propose un outil permettant aux utilisateurs d'altérer automatiquement leurs identités sur les réseaux sociaux comme Facebook, Foursquare ou Twitter[6]. En utilisant cet outil, l'utilisateur accepte de laisser Undefined poster du contenu sur les réseaux sociaux et interagir à sa place avec les autres personnes. Ces actions peuvent être présélectionnées par l'utilisateur parmi une liste de différentes tactiques, censées permettre d'altérer les identités digitales qui sont la proie des algorithmes de surveillance. D'autres projets, comme Vortex[7], proposent notamment aux utilisateurs d'observer comment les algorithmes de profilage réagissent si on fait varier les entrées (inputs) de différentes façons, notamment en jouant avec les cookies. Encore à l'état de prototype, Vortex est une extension de navigateur, conçue comme un *data management game*, permettant aux utilisa-

(1) A. Rouvroy & T. Berns, «Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ?», *Réseaux*, 2013/1 (n° 177), p. 163-196.

(2) G.T. Marx, «A Tack in the Shoe: Neutralizing and Resisting the New Surveillance», *Journal of Social Issues*, Vol. 59, No. 2, 2003, pp. 369-390.

(3) https://www.torproject.org.

(4) J. Pasteur, «La faille et l'exploit : l'activisme informatique», *Cités*, n° 17, 2004, pp. 55-72

(5) F. Brunton & H. Nissenbaum, *Obfuscation. A User's Guide for Privacy and Protest*, MIT Press, 2015. Voir aussi leur article disponible sur Internet en libre accès: «Vernacular resistance to data collection and analysis: A political theory of obfuscation», First Monday, Vol. 16, No. 5, 2 May 2011, http://firstmonday.org/ojs/index.php/fm/rt/printer Friendly/3493/2955.

(6) http://vincentdubois.fr/undefined.php

(7) http://www.milkred.net/vortex

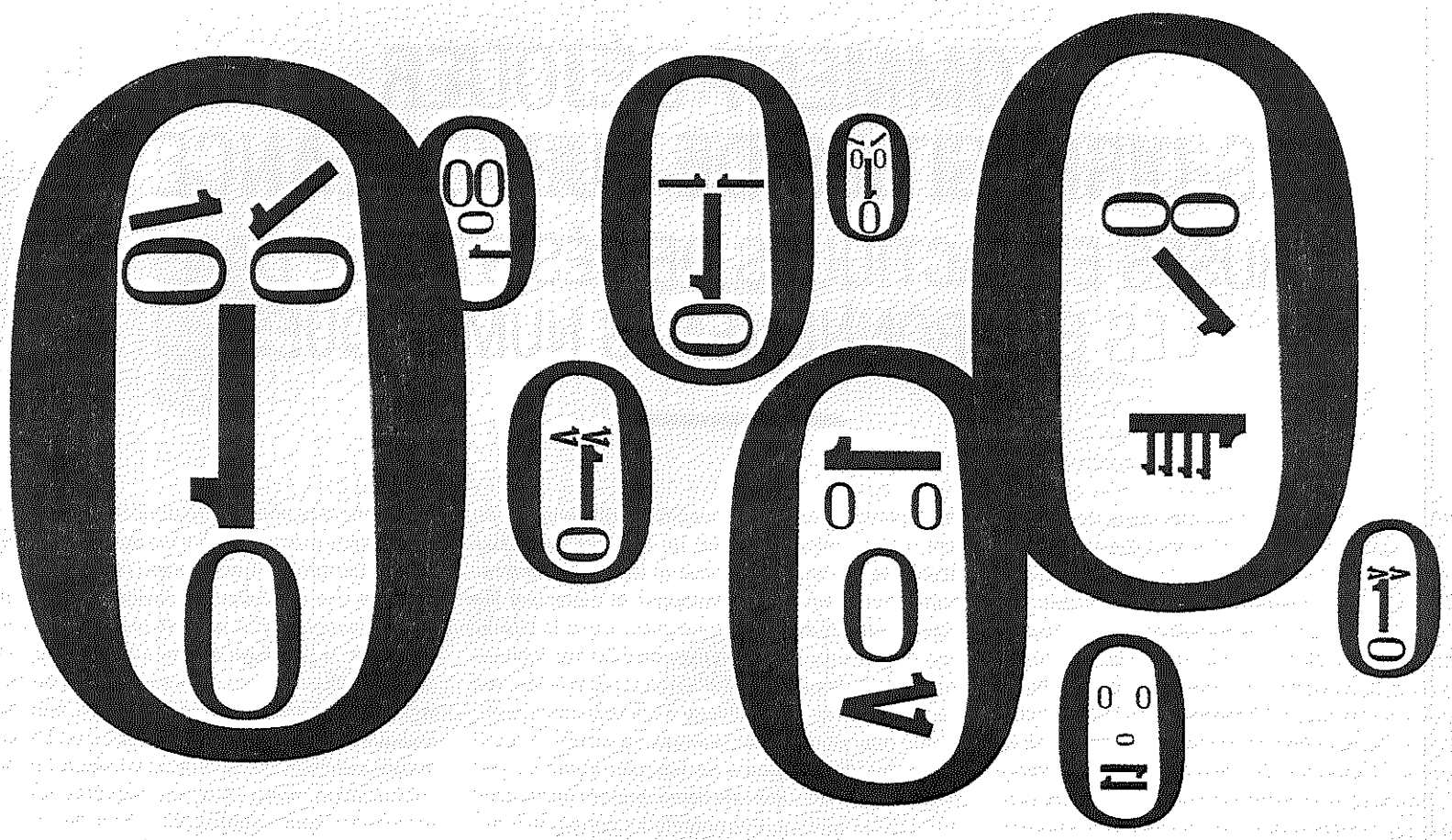


Illustration : Fabienne Loodts

teurs-joueurs de gérer leurs identités digitales en les invitant à échanger les cookies et à observer en temps réel les comportements de leur navigateur en fonction des cookies utilisés. Sur cette base, il devient alors possible de brouiller ses traces et de rendre le profilage moins aisé.

Obfuscation, simulation, diversion, blocage, camouflage… une réelle diversité de tours et de tactiques sont progressivement développés pour tromper les algorithmes traqueurs. Le registre sémantique utilisé par les protagonistes de ces projets lui, par contre, ne trompe pas : il relève de l'art de la guerre ou du combat[9]. La ruse, à travers les stratagèmes qu'elle met en œuvre, s'impose comme une arme servant à déjouer les plans de l'ennemi. Elle est une pratique de résistance qui se situe dans un rapport de force et tente de faire un bon usage des circonstances. La ruse se nourrit donc du conflit et de la rivalité par rapport à une rationalité qui prétend s'imposer sans discussion, fût-elle politique, économique ou techno-scientifique. Dans cette optique, l'engagement tactique et militant des acteurs développant ces différents projets les amène à concevoir des «*contre-artéfacts*»[9] destinés à compenser les situations d'asymétrie ou de déséquilibre structurel auxquelles les utilisateurs de dispositifs numériques (y compris eux-mêmes) sont confrontés en matière de collecte et de traitement de données. Les pratiques rusées qu'ils développent sont des formes de résistance visant à lutter contre la «tyrannie des données» engendrant des situations de faiblesse et de vulnérabilité qu'il s'agit de compenser autant que faire se peut.

Les pratiques rusées développées au sein de ces projets revêtent donc un caractère éminemment politique. En révélant les rouages des dispositifs techniques de profilage, ces projets mettent en évidence les formes spécifiques de subordination qui passent par les choses et qui aujourd'hui désarment particulièrement la critique. En particulier, ces projets mettent en évidence le fait que, dans les environnements numériques, les citoyens ne disposent pas de réelles prises qui leur permettraient d'exercer une éventuelle maîtrise sur leurs données. Alors même qu'on attend de la part du sujet qu'il (re)prenne le contrôle sur ses données, l'environnement dans lequel un tel contrôle est censé s'effectuer n'est absolument pas façonné en ce sens. Les seules prises qu'il offre à l'individu se révèlent être *in fine* les meilleurs moyens d'assurer son emprise. Ainsi en est-il notamment de la fameuse *user-friendliness* des dispositifs et des interfaces constituant le web 2.0, censée faciliter la participation, le partage, l'interactivité et l'autonomie. Les promesses d'aisance et d'interactivité ont inéluctablement comme contrepartie la cession consentie ou involontaire d'informations détaillées à des systèmes toujours plus performants de collecte et d'analyse de données[10].

Compte tenu des situations de déséquilibre profond dans lesquelles sont engagés les utilisateurs, les pratiques rusées, à travers leur «créativité tactique», visent prioritairement à «travailler» les choses afin de se les approprier et de les rendre habitables. Les réflexions de M. de Certeau sont à cet égard précieuses[11]. En effet, pour cet auteur, la tactique, entendue comme la ruse du subalterne, est une façon originale de traiter avec le pouvoir et d'accéder à des ressources. Cela renvoie à une façon de se mouvoir dans un espace qui n'est pas possédé en propre. Les «arts de faire» que nous avons examinés s'apparentent alors à des tentatives pour mieux «faire avec», des arrangements temporaires et provisoires, tirant parti des failles au sein d'un espace strié par des forces indéterminées et démesurées. Dans un tel espace, la ruse ne prémunit pas contre l'incertitude, ni ne garantit la révolution. Tout au plus offre-t-elle une variété d'options pour y naviguer, pour s'en arranger à travers des moyens permettant de rétablir une certaine forme de contrôle…

«*Arme du faible*»[12] visant à s'accommoder au mieux de l'ordre social et de la violence des choses, la ruse aborde la problématique de la vie privée sur un mode agonistique et, ce faisant, contribue à relativiser grandement les fantasmes contemporains sur le contrôle individuel des données. Dans un monde où il devient toujours plus difficile d'effacer ses traces, la ruse est-elle alors la seule solution qu'il nous reste ? L'arme de dernier ressort ? Accepter une telle issue nous semble dangereux car cela reviendrait à réduire trop rapidement l'homme à son animalité, à faire seulement de lui, comme disait Deleuze dans son célèbre abécédaire, un «*être aux aguets*»…

Christophe Lazaro

(8) Voy. aussi G. Deleuze, *Pourparlers* 1971-1990, Les Éditions de Minuit, (1999) 2003, pp. 229-239. Lorsqu'il forge le concept de «société de contrôle», G. Deleuze évoque la nécessité de «*chercher de nouvelles armes*»…

(9) B. Pfaffenberger, *Technological drama*, Sci. Technol. Human Values, Vol. 17, No. 3, 1992, pp. 282-312.

(10) M. Andrejevic, «Privacy, exploitation, and the digital enclosure», *Amsterdam Law Forum*, Vol 1, No 4, 2009, p. 6, http://amsterdamlawforum.org/article/view/94/168.

(11) M. de Certeau, *L'invention du quotidien*, tome 1 : Arts de faire, Gallimard, Paris, 1990.

(12) J. C. Scott, *Weapons of the weak: Everyday forms of peasant resistance*, Yale University Press, New Haven, CT, 1985, p. 29.

(13) http://www.urmesurveillance.com.

(14) https://cvdazzle.com.

(15) http://interventionsjournal.net/2014/03/13/artist-project-facial-weaponization-suite.

LISTE DES PROJETS

- **TrackMeNot**
  http://cs.nyu.edu/trackmenot/fr/
- **AdNauseam**
  http://dhowe.github.io/AdNauseam/
- **Privacy badger**
  https://www.eff.org/privacybadger
- **Undefined**
  http://vincentdubois.fr/undefined.php
- **Are we private yet?**
  http://www.areweprivateyet.com/
- **Adchoices**
  http://www.youronlinechoices.com/ie/your-ad-choices
- **FaceCloak**
  https://crysp.uwaterloo.ca/software/facecloak/
- **Disconnect**
  https://disconnect.me/
- **Vortex**
  http://www.milkred.net/vortex
- **Cryptagram**
  http://cryptogram.prglab.org/
- **Terms of Service; Didn't Read**
  https://tosdr.org/downloads.html

Certains projets revêtent une nature plutôt artistique. Les tactiques de résistance se déploient, par exemple, à travers l'élaboration des masques prothétiques ou des procédés de maquillage-camouflage visant à lutter contre les systèmes de reconnaissance faciale (le projet URME Surveillance[13], CV Dazzle[14], ou le projet Facial Weaponization Suite[15]). Dans ces différents projets, les visages sont défigurés, reconfigurés, voire effacés ; les vertus subversives du masque sont réhabilitées dans un rejet carnavalesque de la surveillance et de l'identification. D'autres initiatives, davantage consacrées aux environnements numériques, démontrent plutôt un caractère techno-militant.

QUE FAUT-IL ENTENDRE PAR « VIRTUALISATION » DE LA SURVEILLANCE ?

Une des caractéristiques des dispositifs de surveillance contemporains est leur nature «numérique». Cette nature procède de processus particuliers, dont les algorithmes[1]. Ils forment le cœur de «briques» technologiques comme les technologies biométriques[2], dont le but est de reconnaître et d'identifier les individus, les technologies de visualisation intelligente (smart CCTV, PTZ, etc) capables de détecter des comportements anormaux, les technologies de localisation, comme les senseurs, capteurs, puces RFID[3], smartphones et autres objets connectés et géolocalisés, et les technologies de *Big Data*, un «*ensemble de technologies, d'architectures, d'outils et de procédures permettant de très rapidement capter, traiter et analyser de larges quantités et contenus hétérogènes et changeants, et d'en extraire les informations pertinentes à un coût accessible*»[4]. Nous pouvons aussi citer, au sein du web 2.0, les réseaux sociaux (comme Facebook), les *cookies*, les services de messagerie et moteurs de recherche gratuits (comme Google), qui tracent et enregistrent nos actes numériques de manière automatique, régulière et intentionnelle.

Une des qualités reconnues à l'ensemble de ces technologies de surveillance serait leur caractère *virtuel*. Elles seraient moins invasives dans la mesure où le contrôle n'est pas «matériel», c'est-à-dire que la surveillance exercée n'est pas toujours matériellement palpable ou ressentie physiquement. La surveillance, rendue invisible, s'allégerait du poids désagréable du contrôle social, tout en étant extrêmement efficace. Une nouvelle forme de surveillance plus légère et moins imposante verrait le jour. Les murs deviendraient invisibles. Comme le soulignent Frank Neisse et Alexandra Novosseloff: «*Constitués d'abord d'obstacles continus de béton ou d'acier scandés à intervalles réguliers de postes de guet, les murs incorporent progressivement de multiples équipements électroniques de détection. Aux États-Unis, des drones munis de caméras infrarouges survolent désormais de manière régulière certaines parties de la frontière. Des tours de surveillance de 30 mètres de haut ont été installées dans les régions désertiques: ce sont des pylônes métalliques élancés sur lesquels sont fixés des caméras et des radars capables de couvrir 45 kilomètres de frontières. Cet ensemble électronique constitue ainsi une sorte de "mur invisible", qui permettra, selon la Border Patrol, de capturer à terme près de 95% des migrants*»[5].

La virtualité qui s'exprime peut alors être perçue comme un adoucissement du contrôle: une sorte de surveillance non-violente, mais efficace et certaine. Il n'en est pourtant rien. A nos yeux, ce phénomène de «virtualisation» de la surveillance constitue au contraire une forme d'extension et d'intensification du pouvoir de surveillance. Dans cet article, notre objectif est de préciser ce qu'il faut entendre par la virtualisation de la surveillance et de rendre compte de ses effets.

QUE FAUT-IL ENTENDRE PAR « VIRTUALISATION » ?

Dans son ouvrage portant sur l'*Histoire politique du barbelé*[6], Olivier Razac met en avant cinq caractéristiques fondamentales de la virtualisation des délimitations des espaces. Bien qu'elle s'applique principalement au fil barbelé, cette technologie constituant selon lui une étape décisive, son analyse permet de penser la virtualisation de la technologie se déployant tant dans une légèreté matérielle que dans une efficacité redoutable. Entre le barbelé et les murs virtuels que constituent les nouvelles technologies de surveillance, il est juste question d'une différence de matière.

1. Virtualisation signifie tout d'abord *effacement matériel*. Alors qu'on pouvait toucher un mur de briques, un mur virtuel est intangible.

2. De plus, l'allègement matériel permet un *gain en mobilité*. Alors qu'un mur de forteresse est difficile à poser et transposer, un mur de fil barbelé se place et se déplace avec une grande facilité et sans coût important.

3. Une telle mobilité permet à son tour une grande *souplesse*. Plutôt qu'une délimitation de l'espace fixe et définitive, un mur virtuel peut suivre les mouvements et les flux. Au contraire de la pierre, «*le fil de métal est une matière élastique qui plie sous l'action d'une force extérieure. Cette action de déformation a pour effet d'absorber l'énergie du choc et d'augmenter la résistance du fil. (...) Souplesse et mobilité se combinent pour permettre une absorption de l'agression de telle manière qu'elle s'enlise en s'affaiblissant progressivement*»[7].

4. Razac souligne également la *discrétion* que rend possible une délimitation virtuelle. Loin d'être l'indice d'une faiblesse, cette discrétion explique la puissance de cette délimitation. Elle évite résistances et oppositions frontales.

5. Enfin, les délimitations virtuelles se caractérisent par leur *réactivité*. Les murs de fil barbelé permettent de ralentir l'agression et de gagner du temps pour réagir.

Olivier Razac définit le concept de virtualisation des délimitations de l'espace à partir de l'étude d'une technologie relativement rudimentaire: le fil barbelé. Il n'est donc pas nécessaire de mobiliser les technologies numériques et de surveillance comme causes déterminantes pour comprendre ce phénomène de «virtualisation». Au contraire, c'est plutôt le sens du rôle de ces technologies qui s'interprète en référence à ce processus de virtualisation.

Dans ses travaux, Jean-Amos Lecat-Deschamps présente précisément la vidéosurveillance comme des murs virtuels[8]. Les caméras sont en effet peu visibles. A l'opposé du mur physique, la caméra ne cherche pas à «bloquer», elle «*n'engendre aucune conséquence physique immédiate*». Elle suit et analyse les flux. De même, elle exerce un effet panoptique dissuasif. Les individus se savent vus, intériorisant en quelque sorte les normes de comportement attendues, ou supposées attendues, du lieu.

UNE GESTION POLITIQUE DE L'ESPACE

Comment cerner ce qui se joue fondamentalement dans ce phénomène de «*virtualisation*»? Il faut éviter d'assimiler virtuel à «moins réel». Comme le souligne Razac, «*la virtualisation ne signifie donc pas un contrôle moindre de l'espace, tout au contraire, l'allégement de la présence en acte des séparations se fait au bénéfice direct de la capacité d'action du pouvoir*»[9]. Il faut comprendre la virtualisation comme une nouvelle forme de «*gestion politique de l'espace*», plutôt qu'une dépolitisation de celle-ci. Il s'agit moins de contrôler l'ouverture et la fermeture de l'espace que de gérer les flux d'un espace ouvert, de «*gérer sa perméabilité*». «*Contrôler les populations sans les freiner*», l'objectif n'étant pas de «*bloquer, mais de faire circuler*»[10]. Il s'agit de gérer ce que Michel Lussault appelle «la trans-spatialité», c'est-à-dire «*l'action spécifique qui consiste à franchir*»[11]. Cette gestion du franchissement et des accès prend appui sur différents protocoles. Lussault évoque à titre emblématique le *filage* ou *queuing*, à savoir une analyse des processus d'optimisation des files d'attente. Il évoque également le *filtrage*, qui «*subordonne un accès à la satisfaction d'une ou de plusieurs vérifications – en général celle des droits de pénétrer dans un lieu et/ou du contenu de ce qu'un individu ou un contenant transporte*»[12]; enfin, le *traçage*, le fait de «*suivre un item entré dans une organisation spatiale et de repérer au moins sa sortie, mieux, ses étapes et sa sortie, mieux encore, tous ses mouvements et ses positions en "temps" réel*»[13].

(1) Voir entre autres Cardon, D., *A quoi rêvent les algorithmes*, Paris, Seuil, 2015; Rouvroy, A. et Berns, T., «Gouvernementalité algorithmique et perspectives d'émancipation», in *Réseaux*, 2013/1, (n° 177), pp. 163-196.

(2) Comme la reconnaissance du visage, la reconnaissance faciale des émotions, la lecture de l'iris, des empreintes digitales, de l'ADN, le body tracking, l'eye tracking... la liste n'est pas exhaustive.

(3) Les puces RFID (de l'anglais radio frequency identification) sont des puces électroniques qui permettent l'identification automatique en utilisant le rayonnement radiofréquence pour identifier les objets porteurs d'étiquettes lorsqu'ils passent à proximité d'un interrogateur.

(4) Voir http://www.redsen-consulting.com/fr/inspired/data-analyse/big-data

(5) Neisse, F. et Novosseloff A., «L'expansion des murs: le reflet d'un monde fragmenté?», in *Politique étrangère* 4/2010 (Hiver), pp. 731-742, p. 736.

(6) Razac, O., *Histoire politique du barbelé*, Paris, Flammarion, 2009.

(7) Razac, O., Ibid., p. 150.

(8) Lecat-Deschamps, J.-A., «La vidéosurveillance, un mur virtuel», in *Hermès*, La Revue 2/2012 (n° 63), pp. 124-129.

(9) Razac, O., Ibid., p. 159.

(10) Ibid., p. 125.

(11) Lussault, M., «Trans-spatialités urbaines», in *Hermès*, La Revue 2/2012 (n° 63), p. 71.

(12) Ibid.

(13) Ibid., p. 72.

Plus encore que le passage ou le franchissement, c'est le *déplacement* lui-même qui devient l'objet du contrôle et de la surveillance. Des dispositifs technologiques dits «intelligents» peuvent détecter automatiquement des comportements jugés anormaux (ou potentiellement anormaux): *«il est possible d'analyser des comportements jugés suspects dans des lieux ouverts ou publics: arrêts fréquents, circulation à contresens, vitesse excessive ou insuffisante, taille du groupe, abandon d'objets, etc. avec tous les croisements possibles entre les différents critères choisis»*[14].

LA BIOMÉTRIE: UN MARQUAGE VIRTUEL DES CORPS

Outre la mise en place d'une véritable gestion politique de l'espace, ces technologies numériques de surveillance ont également pour effet de réaliser un «marquage virtuel» des corps. Elles nous font rentrer dans un régime de biométrie intégrale, dans la mesure où les données captées et agrégées peuvent toujours être reliées à un ou des individus. Nos existences sont continuellement mesurées, comparées, profilées et/ou évaluées.

Remontons brièvement le cours généalogique de la biométrie. Agamben y a apporté une des intuitions premières. Il compara les pratiques biométriques au paradigme politique du camp de concentration, mettant en avant le marquage des corps comme mode d'identification.

«Ainsi, en appliquant au citoyen, ou plutôt à l'être humain comme tel, les techniques et les dispositifs qu'ils avaient inventés pour les classes dangereuses, les États, qui devraient constituer le lieu même de la vie politique, ont fait de lui le suspect par excellence, au point que c'est l'humanité elle-même qui est devenue la classe dangereuse. Il y a quelques années, j'avais écrit que le paradigme politique de l'Occident n'était plus la cité, mais le camp de concentration, et que nous étions passés d'Athènes à Auschwitz. Il s'agissait évidemment d'une thèse philosophique, et non pas d'un récit historique, car on ne saurait confondre des phénomènes qu'il convient au contraire de distinguer. Je voudrais suggérer que le tatouage était sans doute apparu à Auschwitz comme la manière la plus normale et la plus économique de régler l'inscription et l'enregistrement des déportés dans les camps de concentration»[15].

La biométrie réactive la figure du camp de concentration en identifiant rigoureusement corps vivant et identité de la personne, en faisant d'un détail physique un passeport. Mais en même temps, elle procède à cette réactivation dans un esprit entièrement nouveau: en rendant neutre et objective cette naturalisation de l'identité personnelle, et en le concevant simplement comme un moyen pratique, utile, efficace, rapide, elle supprime toute destination infamante ou dégradante du marquage. Ce qui était un marquage infamant devient un mode discret de reconnaissance, auquel il est difficile de s'opposer de manière consciente ou consentante. Les technologies biométriques se présentent dans la neutralité que l'on confère à l'objectivité du chiffre. Par le biais de critères d'identification stables (informatisés et encodés dans un langage universel) et permanents (inscrits dans la permanence du corps), elles apparaissent efficaces, dénuées de toute dérive arbitraire ou de toute considération discriminante.

Toute la force des techniques biométriques réside dans cette «discrétion», ce marquage virtuel, quasi-invisible, quasi-impermanent, comparé à la logique du camp et du tatouage. En plus d'une gestion politique de l'espace et de la perméabilité, c'est également dans une gestion politique des corps qu'il faut comprendre ce phénomène de virtualisation.

Les migrants et les réfugiés révèlent véritablement le sens de cette gestion politique des corps. C'est la biométrie qui permet de vérifier la véracité de leurs récits. Ils sont soumis à une série de tests: tests osseux, de pilosité, de dentition, tests génitaux, en vue de déterminer l'âge *réel* d'une personne se déclarant mineure; mais aussi tests ADN, en vue d'établir la parenté *réelle* entre deux personnes sollicitant le regroupement familial; tests biométriques, pour vérifier l'identité *réelle* d'un individu.

UNE EXTENSION ET UNE INTENSIFICATION DU POUVOIR DE SURVEILLANCE

En conclusion, il est essentiel de réaliser que cette virtualisation ne signifie en rien une atténuation du pouvoir de surveillance, mais qu'il s'agit de l'exercice d'une nouvelle matérialité de ce pouvoir de surveillance, qui lui confère une forme d'extension. Tout d'abord, parce que son objet n'est plus seulement le franchissement de la frontière ou d'une limite, mais le déplacement dans un espace. De plus, l'extension de ce pouvoir n'est pas que spatiale, elle est également temporelle, le but de ces dispositifs «intelligents» étant de détecter des comportements illicites ou anormaux, voire des intentions supposées de comportements répressibles. Comme l'écrit Btihaj Ajana, *«le futur, en tant que tel, est en train progressivement de devenir l'objet de technologie de calcul et de probabilité algorithmique spéculative»*[16]. Deuxièmement, les processus de virtualisation ne signifient en rien «dé-réalisation» des murs et des *frontières.* Au contraire, il s'agit plutôt d'une densification de ces derniers. De plus, il n'est pas rare de constater que loin de remplacer les murs et les frontières physiques, les frontières et murs virtuels se surajoutent aux dispositifs matériels plus classiques. Enfin, la surveillance s'intensifie. Ces critères de normalité tendent à s'intérioriser. Nouvelle forme de pouvoir panoptique, les individus se sachant vus ont tendance à agir selon le comportement normal attendu. Il en résulte des formes de «barrières mentales» (Jean-Amos Lecat-Deschamps), des *«limites intériorisées»* (Philippe Sabot)[17]. Razac cite Michel Lussault à ce sujet: *«Les limites sont souvent mentales et immatérielles, intégrées dans le capital spatial de chaque opérateur, et c'est pourquoi leurs effets sont puissants, car elles demeurent, s'imposent même lorsqu'aucune barrière physique n'existe et organisent la spatialité»*[18].

Nathalie Grandjean et Alain Loute

Respectivement chercheuse senior, responsable de l'Unité Technologies et Sociétés du CRIDS, Université de Namur et chercheur dans le Centre d'éthique médicale, Université Catholique de Lille.

(14) Razac, O., Ibid., p. 220.

(15) Agamben, G., «Non au tatouage biométrique», in *Le Monde*, 10 janvier 2004 (voir http://www.lemonde.fr/archives/article/2004/01/10/non-au-tatouage-biopolitique-par-giorgio-agamben_348677_1819218.html).

(16) Ajana, B., «Augmented borders: Big Data and the ethics of immigration control», in *Journal of Information, Communication and Ethics in Society*, Vol. 13 Iss: 1, 2015, pp. 58-78. Nous traduisons.

(17) «Une société sous contrôle?», in *Methodos* [En ligne], 12 | 2012, URL: http://methodos.revues.org/2941

(18) Lussault, M., *L'homme spatial*, Paris, Seuil, 2007, p. 198, cité in Razac, O., «La matérialité de la surveillance électronique», in *Déviance et société*, 2013/3, Vol. 37, pp. 389-403.

L'AN PIRE RESTE À VENIR